

INTRODUCTION TO LISTING OF THE CLAIMS

In accordance with the PTO's revised amendment format, a detailed listing of all claims has been provided. A status identifier is provided for each claim in parentheses following each claim number. Changes to the claims are shown by strikethrough (for deleted text) or underlining (for added text).

In the Claims:

Claims 1-7, 9-10, 12-22, 24-25, 27-32, 35-37, 39-49, 51-63, 65-77, and 79-81 were previously pending.

Claim 1 is currently amended.

No claims are currently canceled.

No new claims are added.

Pending claims: 1-7, 9-10, 12-22, 24-25, 27-32, 35-37, 39-49, 51-63, 65-77, and 79-81.

Claims:

1. (Currently amended) A method comprising:
generating first and second random values to allow a signature-generating process to generate a signature and additionally encrypt and decrypt a data block;
digitally signing a first string, wherein the first string includes the first random value; and
generating an encryption key for encrypting the data block by hashing a combination of the digitally signed first string and the second random value.
2. (Previously presented) The method as recited in Claim 1, further comprising:
selectively encrypting the data block using the encryption key.
3. (Previously presented) The method as recited in Claim 2, further comprising:
generating a third random value;
obtaining a hash of the third random value; and
including the third random value and the hash of the third random value in the data block to be encrypted.
4. (Previously presented) The method as recited in Claim 3, further comprising decrypting the data block using a decryption key to obtain a decrypted data block, wherein the decrypted data block includes a decrypted third random value and a decrypted hash of the third random value;

obtaining a hash of the decrypted third random value; and
verifying the decryption key by comparing the hash of the decrypted third random value with the decrypted hash of the third random value.

5. (Previously presented) The method as recited in Claim 2, further comprising storing the encrypted data block, the first random value and the second random value.

6. (Previously presented) The method as recited in Claim 5, further comprising:

accessing the stored encrypted data block, the stored first random value and the stored second random value;

digitally signing a second string, wherein the second string includes the stored first random value; and

generating a decryption key by hashing a combination of the digitally signed second string and the stored second random value.

7. (Previously presented) The method as recited in Claim 5, wherein the encrypted data block, the first random value and the second random value are each stored on a storage medium.

8. (Canceled)

9. (Previously presented) The method as recited in Claim 1, wherein generating the encryption key further includes cryptographically hashing the digitally signed first string concatenated with the second random value.

10. (Previously presented) The method as recited in Claim 1, wherein generating the encryption key further includes cryptographically hashing the second random value concatenated with the digitally signed first string.

11. (Canceled)

12. (Previously presented) The method as recited in Claim 1, wherein a first device generates the first random value, the second random value, and the encryption key.

13. (Previously presented) The method as recited in Claim 1, wherein a second device digitally signs the first string.

14. (Previously presented) The method as recited in Claim 13, wherein the second device comprises a signature-generating device.

15. (Previously presented) The method as recited in Claim 14, wherein the signature-generating device comprises a smart card.

16. (Previously presented) A computer-readable medium having computer-executable instructions for performing steps comprising:

generating first and second random values to allow a signature-generating process to participate in encrypting and decrypting a data block;

digitally signing a string that includes the first random value; and

generating an encryption key based on the digitally signed string and the second random value.

17. (Previously presented) The computer-readable medium as recited in Claim 16, further comprising computer-executable instructions for:

selectively encrypting the data block using the encryption key.

18. (Previously presented) The computer-readable medium as recited in Claim 17, further comprising instructions for:

generating a third random value;

hashing the third random value; and

including the third random value and the hash of the third random value in the data block.

19. (Previously presented) The computer-readable medium as recited in Claim 18, further comprising instructions for:

decrypting the data block using a decryption key to obtain a decrypted data block, wherein the decrypted data block includes a decrypted third random value and a decrypted hash of the third random value;

obtaining a hash of the decrypted third random value; and
verifying the decryption key by comparing the hash of the decrypted third random value with the decrypted hash of the third random value.

20. (Previously presented) The computer-readable medium as recited in Claim 17, further comprising computer-executable instructions for:

storing the encrypted data block, the first random value and the second random value.

21. (Previously presented) The computer-readable medium as recited in Claim 20, further comprising computer-executable instructions for:

accessing the stored encrypted data block, the stored first random value and the stored second random value;

digitally signing a second string, wherein the second string includes the stored first random value; and

generating a decryption key by hashing a combination of the digitally signed second string and the stored second random value.

22. (Previously presented) The computer-readable medium as recited in Claim 20, wherein the encrypted data block, the first random value and the second random value are each stored on a storage medium.

23. (Canceled)

24. (Previously presented) The computer-readable medium as recited in Claim 16, wherein generating the encryption key further includes cryptographically hashing the digitally signed string concatenated with the second random value.

25. (Previously presented) The computer-readable medium as recited in Claim 16, wherein generating the encryption key further includes cryptographically hashing the second random value concatenated with the digitally signed string.

26. (Canceled)

27. (Previously presented) The computer-readable medium as recited in Claim 16, wherein the first random value and the second random value are each generated by a first device that is configured to generate the encryption key.

28. (Previously presented) The computer-readable medium as recited in Claim 16, wherein a second device digitally signs the string.

29. (Original) The computer-readable medium as recited in Claim 28, wherein the second device includes a signature-generating device.

30. (Original) The computer-readable medium as recited in Claim 29, wherein the signature-generating device is a smart card.

31. (Previously presented) An arrangement comprising:

first logic configured to selectively hash a first data string, wherein the first data string and the hash of the first data string are to be included in a data block to be encrypted by a signature-generating process;

second logic operatively coupled to the first logic and configured to digitally sign a second data string; and

wherein the first logic is further configured to generate an encryption key based on a combination of the digitally signed second data string and a third data string.

32. (Previously presented) The arrangement as recited in Claim 31, wherein the first logic is further configured to selectively encrypt the data block using the encryption key.

33. (Canceled)

34. (Canceled)

35. (Previously presented) The arrangement as recited in Claim 32, wherein the first logic is further configured to store the encrypted data, the second data string and the third data string.

36. (Previously presented) The arrangement as recited in Claim 35, further including memory operatively coupled to the first logic, wherein the first logic stores the encrypted data, the second data string and the third data string are in the memory.

37. (Original) The arrangement as recited in Claim 35, further including a data storage device having at least one storage medium, the data storage device being operatively coupled to the first logic, and wherein the first logic provides the encrypted data, the second data string and the third data string to the storage device for storage on a storage medium.

38. (Canceled)

39. (Previously presented) The arrangement as recited in Claim 31, wherein the first logic is further configured to cryptographically hash the digitally signed second data string concatenated with the third data string.

40. (Previously presented) The arrangement as recited in Claim 31, wherein the first logic is further configured to cryptographically hash the third data string concatenated with the digitally signed second data string.

41. (Previously presented) The arrangement as recited in Claim 31, wherein at least one data string selected from among the first data string, the second data string and the third data string includes a randomly generated data string.

42. (Original) The arrangement as recited in Claim 31, wherein the first data string, the second data string and the third data string are each generated by the first logic.

43. (Original) The arrangement as recited in Claim 31, wherein the second logic is provided within a smart card.

44. (Previously presented) A method comprising:
generating first, second, and third data strings;
digitally signing the second data string; and
generating an encryption key for encrypting a data block based on the digitally signed second data string and the third data string;
encrypting the data block using the encryption key; and
storing the encrypted data block, the second data string, and the third data string.

45. (Previously presented) The method as recited in Claim 44, further comprising:

accessing the stored encrypted data block, the stored second data string, and the stored third data string;

digitally signing the second data string accessed from storage;

generating a decryption key based on the digitally signed second data string and the third data string accessed from storage; and

decrypting the encrypted data block using the decryption key.

46. (Previously presented) The method as recited in Claim 45, wherein the resulting decrypted data block includes the first data string.

47. (Previously presented) The method as recited in Claim 46, wherein the resulting decrypted data block includes a hash of the first data string.

48. (Previously presented) The method as recited in Claim 45, wherein the accessing further includes reading a memory.

49. (Previously presented) The method as recited in Claim 45, wherein the accessing further includes reading data from at least one storage medium.

50. (Canceled)

51. (Previously presented) The method as recited in Claim 44, wherein generating the encryption key further includes cryptographically hashing the digitally signed second data string concatenated with the third data string.

52. (Previously presented) The method as recited in Claim 44, wherein generating the encryption key further includes cryptographically hashing the third data string concatenated with the digitally signed second data string.

53. (Previously presented) The method as recited in Claim 44, wherein at least one data string selected from among the first data string, the second data string and the third data string includes a randomly generated data string.

54. (Original) The method as recited in Claim 44, wherein the first data string, the third data string, and the encrypted data are each accessed by a first device that is configured to selectively hash the first data string and generate the encryption key.

55. (Original) The method as recited in Claim 44, wherein a second device digitally signs the second data string.

56. (Original) The method as recited in Claim 55, wherein the second device includes a signature-generating device.

57. (Original) The method as recited in Claim 56, wherein the signature-generating device is a smart card.

58. (Previously presented) A computer-readable medium having computer-executable instructions for performing steps comprising:

accessing from storage first, second, and third data strings;

digitally signing the second data string;

generating an encryption key based on the digitally signed second data string and the third data string; and

encrypting a data block using the encryption key.

59. (Previously presented) The computer-readable medium as recited in Claim 58, further comprising computer-readable medium having computer-executable instructions for:

accessing the encrypted data block; and

decrypting the encrypted data block using the encryption key.

60. (Previously presented) The computer-readable medium as recited in Claim 59, wherein the resulting decrypted data block includes the first data string.

61. (Previously presented) The computer-readable medium as recited in Claim 60, wherein the resulting decrypted data block includes a hash of the first data string.

62. (Previously presented) The computer-readable medium as recited in Claim 59, wherein the accessing includes reading a memory.

63. (Previously presented) The computer-readable medium as recited in Claim 59, wherein the accessing includes reading data from at least one storage medium.

64. (Canceled)

65. (Previously presented) The computer-readable medium as recited in Claim 58, wherein generating the encryption key further includes cryptographically hashing the digitally signed second data string concatenated with the third data string.

66. (Previously presented) The computer-readable medium as recited in Claim 58, wherein generating the encryption key further includes cryptographically hashing the third data string concatenated with the digitally signed second data string.

67. (Previously presented) The computer-readable medium as recited in Claim 58, wherein at least one data string selected from among the first data string, the second data string and the third data string includes a randomly generated data string.

68. (Original) The computer-readable medium as recited in Claim 58, wherein the first data string, the third data string, and the encrypted data are each accessed by a first device that is configured to selectively hash the first data string and generate the encryption key.

69. (Original) The computer-readable medium as recited in Claim 58, wherein a second device digitally signs the second data string.

70. (Previously presented) The computer-readable medium as recited in Claim 69, wherein the second device performs a signature-generating process.

71. (Previously presented) The computer-readable medium as recited in Claim 70, wherein a smart card performs the signature-generating process.

72. (Previously presented) A system comprising:
a data block to be encrypted by an encryption key;
a first device capable of generating the encryption key;
a second device capable of digitally signing a string;
first logic associated with the first device to generate first, second, and third data strings;
second logic associated with the second device to digitally sign the second data string; and
at least a part of the first logic further configured to generate the encryption key based on the digitally signed second data string and the third data string.

73. (Previously presented) The system as recited in Claim 72, wherein the first logic is further configured to:

encrypt the data block;

store the encrypted data block, the second data string, and the third data string;

access the encrypted data block, the second data string, and the third data string from storage;

obtain a signed second data string from the second device;

regenerate the encryption key from the signed second data string and the third data string; and

decrypt the encrypted data block using the regenerated encryption key.

74. (Previously presented) The system as recited in Claim 73, wherein the resulting decrypted data block includes the first data string.

75. (Previously presented) The system as recited in Claim 74, wherein the resulting decrypted data block includes a hash of the first data string, and the first logic verifies the regenerated encryption key by hashing the first data string from the decrypted data block and comparing the hash of the decrypted first data string with the hash of the first data string obtained from the decrypted data block.

76. (Previously presented) The system as recited in Claim 73, further comprising memory operatively coupled to the first logic, and wherein the first logic reads the plurality of stored data strings and the encrypted data block from the memory.

77. (Previously presented) The system as recited in Claim 73, further comprising a data storage device having at least one storage medium, and wherein the first logic reads the plurality of stored data strings and the encrypted data block from the storage medium.

78. (Canceled)

79. (Previously presented) The system as recited in Claim 72, wherein the first logic is further configured to generate the encryption key by cryptographically hashing the digitally signed second data string concatenated with the third data string.

80. (Previously presented) The system as recited in Claim 72, wherein the first logic is further configured to generate the encryption key by cryptographically hashing the third data string concatenated with the digitally signed second data string.

81. (Previously presented) The system as recited in Claim 72, wherein at least one data string selected from among the first data string, the second data string and the third data string includes a randomly generated data string.

82. (Canceled)